General Data Protection Regulations

Factsheet for UNISON members

General Data Protection Regulations

UNISON

Introduction

The General Data Protection Regulations (GDPR) give individuals more choice and control over how their data is used.

This factsheet is designed to help you feel confident about how you use and protect data as you go about your work.

The regulations include strict duties, which all organisations must follow. Failure to comply with legislation could result in heavy fines, therefore compliance with the regulations is essential.

All staff have a responsibility to ensure that their own activities comply with GDPR.

What you need to know at work

- GDPR covers all processing of personal data. It applies to any personal data that is processed about service users, staff members (such as HR records), or other interested parties.
- Your organisation will have someone with designated responsibility for data protection matters, including GDPR. They will be responsible for ensuring that personal data is correctly collected, stored, used and securely destroyed once it is no longer needed.
- Your organisation needs to have robust procedures to deal with data protection breaches. A data breach is anything leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data. Most breaches are the result of human error. They are rarely malicious. Under GDPR, certain breaches will need to be reported to the Information Commissioner's Office (ICO). Your employer should have a procedure for this.
- You should never disclose any personal data outside of your organisation's procedures, or use personal data held on others for your own purposes. Doing so is a breach of GDPR and possibly a criminal offence.
- You should take extra care to ensure that any personal data you use at work is kept secure. This doesn't need to be complicated or expensive, it is just a case of treating other people's data as you would your own. Actions to consider are:
  - Keeping files in locked cabinets.
  - Using a shredder or a confidential waste bin where data is no longer needed.
  - Having a clear desk policy.
  - Locking your computer screen when you are away from your desk.
  - Encrypting removable media, USBs (memory sticks), CDs etc so that if they are lost the data cannot be accessed.
  - Taking care if working in public – people may be able to see your screen.

What is a data controller?

A ‘data controller’ is the organisation which determines how your data is processed e.g. your employer. Under GDPR, a controller must:

- Be transparent and tell you how your personal data will be used.
- Tell you if they intend to share your data, so that you can decide whether you want to participate.
- Only ask you for data that is necessary and not for anything excessive.
- Inform you how long they intend to keep your data.

Your individual rights

- It is important to be aware of your rights as a ‘data subject’. You have:
- “The right to be informed” – you must be informed how an organisation is going to use your personal data.
- “The right of access” – you have the right to access your personal data that an organisation holds. This is called a “subject access request”.
- “The right to rectification” – you have the right to inform an organisation if you think the data they hold on you is incorrect so that they can put it right.
- “The right to erasure” – you have the right to request that an organisation deletes your data, if they no longer need it.
- “The right to restrict processing” – in certain circumstances, you have the right to restrict how an organisation processes your data, for example restricting how they can contact you.
- “The right to data portability” – you can obtain and reuse your personal data for your own purposes across different services e.g. different unions.

Children’s data under GDPR

- The GDPR includes special protections in relation to children’s data. This is mostly focused on allowing children to make informed decisions as to how their data will be processed, for example when they are using social media.
- Children have the same rights under GDPR as adults. This includes the right to make a subject access request.
- Compliance with data protection regulations, including GDPR, should be central to all processing of children’s personal data.

When things go wrong…

Data breaches are nearly always the result of human error. The most common data breaches are:

- Paper files or USB sticks are lost.
- An email containing personal data is sent to the wrong person in error. Sometimes the incorrect recipient will have the same name as the intended recipient.
- An email is sent to a group of people using the CC field rather than the BCC field, therefore disclosing everyone's email address to everyone else.
- Personal data is left on desks unsecured.
- An incorrect document containing personal data is attached to an email in error.

…don't panic!

If you have made an error like those above, don't panic! You should follow your employer's breach reporting procedure immediately. If they do not have a breach reporting procedure, tell your line manager about the breach instead. Delaying reporting the incident will only make matters worse.

Once you have reported the breach, you can also contact your UNISON branch for advice.

Further questions

If you have concerns that your employer has misused information, or has not kept it secure and safe enough, you can contact your UNISON branch for advice.

If you want more expert advice, join UNISON.

Join today at **joinunison.org** or call **0800 171 2193** or ask your UNISON rep for an application form.

Published and printed by UNISON, UNISON Centre, 130 Euston Road, London NW1 2AY.
CU/May 2018/25018/3959/UNP 15121.